

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Seigo KOTANI et al.

Group Art Unit:

Serial No.:

Examiner:

Filed: December 20, 2000

For: CRYPTOGRAPHIC COMMUNICATION METHOD, FILE ACCESS
SYSTEM AND RECORDING MEDIUM



**SUBMISSION OF CERTIFIED COPY OF PRIOR
FOREIGN APPLICATION IN ACCORDANCE WITH
THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application(s):

Japanese Patent Application No. 2000-16657
Filed: January 26, 2000

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing
date, as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: December 20, 2000

By: _____


H. J. Staas
Registration No. 22,010

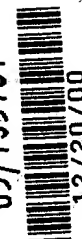
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

JC945 U.S. PTO

09/739757



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 1月26日

出 願 番 号
Application Number:

特願2000-016657

出 願 人
Applicant (s):

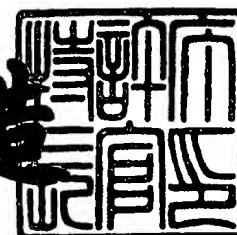
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年10月 6日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



【書類名】 特許願

【整理番号】 9995327

【提出日】 平成12年 1月26日

【あて先】 特許庁長官殿

【国際特許分類】 H04K 1/00

【発明の名称】 暗号通信方法およびファイルアクセスシステム並びに記録媒体

【請求項の数】 14

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【発明者】

 【住所又は居所】 東京都港区芝浦四丁目15番33号 株式会社富士通ビー・エス・シー内

 【氏名】 佐々木 孝興

【発明者】

 【住所又は居所】 東京都港区芝浦四丁目15番33号 株式会社富士通ビー・エス・シー内

 【氏名】 山中 祐介

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 長谷部 高行

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 秋山 良太

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100086933

【弁理士】

【氏名又は名称】 久保 幸雄

【電話番号】 06-6304-1590

【手数料の表示】

【予納台帳番号】 010995

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704487

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号通信方法およびファイルアクセスシステム並びに記録媒体

【特許請求の範囲】

【請求項 1】

送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信方法であって、

送信側において、前記通信用の鍵とは異なる個別用の鍵で暗号化されたデータを送信するに当たり、前記暗号化されたデータを、前記個別用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵を用いて暗号化して送信する、

ことを特徴とする暗号通信方法。

【請求項 2】

前記通信用の鍵を用いて暗号化する際に、元のデータのファイル識別子をファイル名に組み込み、暗号化されたデータであることを示す識別子を新たに付加する、

請求項 1 記載の暗号通信方法。

【請求項 3】

送信側において鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、

受信側において、受信したデータを、前記通信用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵とは異なる個別用の鍵で暗号化して記憶するとともに、前記復号化されたデータを削除する、

ことを特徴とする暗号通信方法。

【請求項 4】

前記個別用の鍵および前記通信用の鍵による暗号化または復号化を可能にするために、前記個別用の鍵および前記通信用の鍵に対してそれぞれ個別に認証を行う、

請求項 1 ないし請求項 3 のいずれかに記載の暗号通信方法。

【請求項 5】

送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、

送信側において暗号化を行う際に、暗号化に用いた通信用の鍵に対応する識別コードを、暗号化されたデータに付加し、

受信側において、前記識別コードに対応した通信用の鍵を用いて復号化する、ことを特徴とする暗号通信方法。

【請求項 6】

送信側において通信用の鍵を複数個準備しておき、それらのうちの 1 つの鍵を用いてデータを暗号化するとともに、暗号化に用いた鍵に対応する識別コードを暗号化されたデータに付加する、

請求項 5 記載の暗号通信方法。

【請求項 7】

受信側において通信用の鍵を複数個準備しておき、それらのうちの前記識別コードに対応した通信用の鍵を選択して用いる、

請求項 5 記載の暗号通信方法。

【請求項 8】

互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とし、1 つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う、

ことを特徴とするファイルアクセスシステム。

【請求項 9】

互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とし、処理対象のファイルが暗号化されているか否かを判別し、暗号化されている場合に一方の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、

続いて、暗号化されていないファイルを他方の鍵を用いて暗号化する、

ことを特徴とするファイルアクセスシステム。

【請求項 10】

互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とし、暗号化されているファイルを一方の鍵を用いて復号化し、

ファイルの格納先が暗号化ファイル用であるか否かを判別し、暗号化ファイル用である場合に前記ファイルを他方の鍵で暗号化して格納し、暗号化ファイル用でない場合に前記ファイルをそのまま格納する、

ことを特徴とするファイルアクセスシステム。

【請求項 1 1】

第 1 のホルダおよび第 2 のホルダを示す画面を表示し、

前記第 1 のホルダに格納されたファイルを前記第 2 のホルダに移動する指示入力があったときに、前記第 1 のホルダに格納されたファイルの復号化および／または暗号化を行い、復号化および／または暗号化されたファイルを前記第 2 のホルダに格納する、

ことを特徴とするファイルアクセスシステム。

【請求項 1 2】

前記第 1 のホルダに格納されたファイルが暗号化されているか否かを判別し、暗号化されている場合に第 1 の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、

続いて、暗号化されていないファイルを第 2 の鍵を用いて暗号化する、

請求項 1 1 記載のファイルアクセスシステム。

【請求項 1 3】

ファイルへのアクセスのためのプログラムを記録した記録媒体であって、

互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とする処理と、

1 つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う処理と、

をコンピュータに実行させるためのプログラムを格納したコンピュータ読み取り可能な記録媒体。

【請求項 1 4】

送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信に用いられる暗号化処理装置であって、

前記通信用の鍵と、

前記通信用の鍵とは異なる個別用の鍵と、

前記個別用の鍵による復号化および前記通信用の鍵による暗号化を連続的に行う処理部とを有してなる、

ことを特徴とする暗号化処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、暗号通信方法およびファイルアクセスシステム並びに記録媒体に関する。

【0002】

パーソナルコンピュータが普及し、パソコン通信または電子メールなどのネットワークを介した通信が業務上欠かせないものとなっている。個別のパーソナルコンピュータで用いるデータのみでなく、それらのデータをネットワークを介して通信することをも考慮して、データのセキュリティの保護を総合的に図る必要がある。

【0003】

【従来の技術】

従来において、電子メールなどで通信を行うデータのセキュリティの保護のために、鍵を用いてデータを暗号化して送信し、受信側において受信したデータを送信側と共通の鍵を用いて復号化する通信方法が知られている。

【0004】

一方、パーソナルコンピュータで扱うファイルのセキュリティの保護のためのファイルアクセスシステムを、本出願人は特開平10-301856号として提案した。これによると、認証により使用権限が確認されて鍵が活性化されている間において、任意のファイルを指定のホルダに入れるとそれが自動的に暗号化され、且つそのホルダ内のファイルを読み出す際には自動的に復号化される。使用権限を有するユーザは、暗号化されたファイルを通常のファイルと同じように閲覧し編集することができ、ファイルが暗号化されていることを全く意識する必要

がない。

【0005】

【発明が解決しようとする課題】

上に述べたファイルアクセスシステムは、個人用のコンピュータの内部において、データベースまたはファイルなどの種々のコンテンツ類を扱うのに非常に優れたシステムである。

【0006】

しかしながら、自分のコンテンツを暗号化して他者に送信したい場合、または他者から送信された暗号化コンテンツを個人用の鍵で暗号化して運用したい場合などにおいて、そのままでは不都合が生じる。

【0007】

つまり、例えば、暗号化されたコンテンツを電子メールの添付ファイルとして送信する場合に、添付ファイルとするためのリード命令によって添付ファイルが自動的に復号化されてしまう。これを防ぐには、鍵の機能を事前に停止させる必要があるが、そのための操作が煩雑であるので、暗号化されていない添付ファイルを誤って送信してしまうおそれがある。

【0008】

また、暗号化されていないコンテンツを暗号化した添付ファイルとして送信する場合に、鍵を活性化して一旦暗号化を行い、その後に鍵の機能を停止させた上で、リード命令によって添付ファイルとする必要がある。この場合も操作が煩雑であり、操作を誤って復号化された添付ファイルを送信してしまう可能性がある。

【0009】

本発明は、上述の問題に鑑みてなされたもので、暗号化されたデータおよび暗号化されていないデータを混在して扱う場合などにおいて、容易な操作で間違ふことなく暗号通信を行えるようにすることを目的とする。

【0010】

【課題を解決するための手段】

請求項1の発明に係る方法は、送信側において通信用の鍵を用いてデータを暗

号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信方法であって、送信側において、前記通信用の鍵とは異なる個別用の鍵で暗号化されたデータを送信するに当たり、前記暗号化されたデータを、前記個別用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵を用いて暗号化して送信する。

【 0 0 1 1 】

請求項 2 の発明に係る方法では、前記通信用の鍵を用いて暗号化する際に、元のデータのファイル識別子をファイル名に組み込み、暗号化されたデータであることを示す識別子を新たに付加する。

【 0 0 1 2 】

請求項 3 の発明に係る方法は、送信側において鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、受信側において、受信したデータを、前記通信用の鍵を用いて復号化し、続いて、復号化されたデータを前記通信用の鍵とは異なる個別用の鍵で暗号化して記憶するとともに、前記復号化されたデータを削除する。

【 0 0 1 3 】

請求項 4 の発明に係る方法では、前記個別用の鍵および前記通信用の鍵による暗号化または復号化を可能にするために、前記個別用の鍵および前記通信用の鍵に対してそれぞれ個別に認証を行う。

【 0 0 1 4 】

請求項 5 の発明に係る方法は、送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを通信用の鍵を用いて復号化する暗号通信方法であって、送信側において暗号化を行う際に、暗号化に用いた通信用の鍵に対応する識別コードを、暗号化されたデータに付加し、受信側において、前記識別コードに対応した通信用の鍵を用いて復号化する。

【 0 0 1 5 】

請求項 6 の発明に係る方法では、送信側において通信用の鍵を複数個準備しておき、それらのうちの 1 つの鍵を用いてデータを暗号化するとともに、暗号化に用いた鍵に対応する識別コードを暗号化されたデータに付加する。

【 0 0 1 6 】

請求項 7 の発明に係る方法では、受信側において通信用の鍵を複数個準備しておき、それらのうちの前記識別コードに対応した通信用の鍵を選択して用いる。

請求項 8 の発明に係るシステムは、互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とし、1 つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う。

【 0 0 1 7 】

請求項 9 の発明に係るシステムは、互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とし、処理対象のファイルが暗号化されているか否かを判別し、暗号化されている場合に一方の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、続いて、暗号化されていないファイルを他方の鍵を用いて暗号化する。

【 0 0 1 8 】

請求項 1 0 の発明に係るシステムは、互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とし、暗号化されているファイルを一方の鍵を用いて復号化し、ファイルの格納先が暗号化ファイル用であるか否かを判別し、暗号化ファイル用である場合に前記ファイルを他方の鍵で暗号化して格納し、暗号化ファイル用でない場合に前記ファイルをそのまま格納する。

【 0 0 1 9 】

請求項 1 1 の発明に係るシステムは、第 1 のホルダおよび第 2 のホルダを示す画面を表示し、前記第 1 のホルダに格納されたファイルを前記第 2 のホルダに移動する指示入力があったときに、前記第 1 のホルダに格納されたファイルの復号化および／または暗号化を行い、復号化および／または暗号化されたファイルを前記第 2 のホルダに格納する。

【 0 0 2 0 】

請求項 1 2 の発明に係るシステムは、前記第 1 のホルダに格納されたファイルが暗号化されているか否かを判別し、暗号化されている場合に第 1 の鍵を用いて復号化し、暗号化されていない場合にはそのままとし、続いて、暗号化されていないファイルを第 2 の鍵を用いて暗号化する。

【 0 0 2 1 】

請求項 1 3 の発明に係る記録媒体は、ファイルへのアクセスのためのプログラムを記録した記録媒体であって、互いに異なる 2 つの鍵をそれぞれ個別に認証することによって使用可能とする処理と、1 つのファイルに対して、一方の鍵による復号化および他方の鍵による暗号化を連続的に行う処理と、をコンピュータに実行させるためのプログラムを格納したコンピュータ読み取り可能な記録媒体である。

【 0 0 2 2 】

請求項 1 4 の発明に係る装置は、送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを鍵を用いて復号化する暗号通信に用いられる暗号化処理装置であって、前記通信用の鍵と、前記通信用の鍵とは異なる個別用の鍵と、前記個別用の鍵による復号化および前記通信用の鍵による暗号化を連続的に行う処理部とを有してなる。

【 0 0 2 3 】

本発明において、送信側において用いられる通信用の鍵と、受信側において用いられる通信用の鍵とは、共通の同じ鍵であってもよいし、また、互いに異なる別の鍵であってもよい。

【 0 0 2 4 】

【発明の実施の形態】

図 1 は通信システム 1 の例を示すブロック図、図 2 は暗号化カード S P C の構成を示すブロック図、図 3 はグループ鍵による暗号化処理を行う前後のファイルの状態を示す図である。

【 0 0 2 5 】

図 1 において、通信システム 1 は、ネットワーク NW に接続された複数の通信端末 5 a, 5 b, … からなる。ネットワーク NW は、LAN、WAN、公衆回線、専用回線、無線回線、またはインターネットなど、若しくはそれらの組み合わせによるネットワークである。また、複数のネットワークを介したネットワーク NW であってもよい。通信端末 5 a, 5 b, … として、例えばパーソナルコンピュータを用いることができ、その構成の一例が図に示されている。以降において

、通信端末 5 a, 5 b, …のいずれかかまたは全体を指して「通信端末 5」と記載することがある。

【 0 0 2 6 】

通信端末 5 は、処理装置 1 1、表示装置 1 2、ドライブ装置 1 3、入力装置 1 4、暗号化カード S P C、その他の装置から構成される。

処理装置 1 1 は、C P U、R O M、主メモリ、外部記憶装置、通信制御回路、種々のインタフェース、その他の周辺回路などを備え、他の装置、特に暗号化カード S P C とも協働して本発明に係る暗号通信のための処理、ファイルアクセス処理、その他の種々の処理を行う。外部記憶装置には、本発明に係る暗号通信のためのアプリケーションプログラム、他のプログラム、種々のファイル、テーブル、データベース、その他のデータが記憶される。

【 0 0 2 7 】

表示装置 1 2 は、その表示面 H G に、画像、文字、および後述する種々の画面を表示する。

ドライブ装置 1 3 は、C D - R O M (C D)、フロッピーディスク F D、または光磁気ディスクなどの記録媒体がセットされたときに、それにアクセスしてデータまたはプログラムの読み書きを行う。

【 0 0 2 8 】

入力装置 1 4 は、キーボード、マウス、または他のポインティングデバイスなどであり、データを入力しまたは処理装置 1 1 に指令を与えるために用いられる。

【 0 0 2 9 】

図 2 に示すように、暗号化カード S P C は、暗号化処理部 2 1、復号化処理部 2 2、および鍵部 3 2 を備える。

鍵部 3 2 には、多数の鍵 K 1, K 2, K 3 …が格納されている。図では 1 2 個の鍵 K が示されているが、それ以下であってもよく、またそれ以上、例えば 1 6 個であってもよい。これらの各鍵 K は、それぞれの識別コードと対応付けられている。暗号化カード S P C を使用する際には、その起動時に使用権限を確認するための認証が行われるが、その際に入力されるユーザ I D またはグループ I D が

その識別コードに対応し、それと一致する鍵Kが選択されるようになっている。
ユーザID（個別ID）により選択される鍵Kは個別鍵KPとして機能し、グループIDにより選択される鍵Kはグループ鍵KGとして機能する。

【0030】

なお、この例の実施形態においては、暗号通信を行う場合に、送信側および受信側において、少なくとも1つの共通の鍵Kを持っておく必要がある。

暗号化処理部21および復号化処理部22は、鍵部32から選択された鍵Kを用いて、暗号化処理または復号化処理を行う。これらの処理は可逆処理である。つまり、暗号化処理を行った後に復号化処理を行うことにより、またその逆を行うことにより、元の状態に戻る。このときの処理の例の詳細は、上に述べた特開平10-301856号を参照することができる。

【0031】

但し、グループ鍵KGによる暗号化処理または復号化処理を行う場合には、元のデータに対して、ヘッダを付加しまたは削除する処理が行われる。

すなわち、例えば、図3（A）に示すように、ヘッダHD、本文BD、フッタFO、からなる1つのファイルFL1があった場合に、グループ鍵KGを用いてこの暗号化処理を行うと、図3（B）に示すように、ファイルFL1の全体が暗号化されて本文CBDとなり、これに新たなヘッダCHDが付加されたファイルFL2となる。その際に、グループ鍵KGに対応する識別コード（グループID）が属性情報としてヘッダCHDに付加される。グループ鍵KGを用いてファイルFL2の復号化処理を行うと、ファイルFL1に戻る。

【0032】

なお、暗号化カードSPCは、本実施形態においてはPCカードの形態で用いられるが、他の形態であってもよい。また、本実施形態においては暗号化カードSPCによって暗号化処理および復号化処理を行っているが、暗号化カードSPCを用いることなく、同様の処理をソフトウェアによって実行することも可能である。

【0033】

図4は通信端末5a、5bの暗号通信時における機能を示すブロック図である

。なお、図4においては、通信端末5aを送信側とし、通信端末5bを受信側としてあるが、各通信端末5によって送信および受信のいずれをも行うことができる。

【0034】

図4において、送信側の通信端末5aは、暗号ホルダFA、平文ホルダFH、送受信ホルダFT、および暗号化カードSPCを有する。

暗号ホルダFAは、それが活性化されているときに、他のホルダから暗号ホルダFAにファイルを移動した際に、自動的にそのファイルの暗号化処理が行われ、暗号化されたファイル（暗号ファイル）として暗号ホルダFAに格納される。また、暗号ホルダFAに格納されているファイル（暗号ファイル）を、暗号ホルダFAから他のホルダに移動した際には、自動的にそのファイルの復号化処理が行われ、復号化されたファイル（平文ファイル）として移動先のホルダに格納される。

【0035】

つまり、暗号ホルダFAに入ってくる際には暗号化処理が行われ、暗号ホルダFAから出ていく際には復号化処理が行われる。この際に、移動するファイルの種類は問わない。例えばそれが暗号ファイルであっても平文ファイルであってもよい。例えば、もし暗号ファイルが暗号ホルダFAに入ってくると、再度の暗号化処理が行われ、これは復号化処理を2回行うことによって平文ファイルに戻すことができる。

【0036】

そして、暗号ホルダFAに格納された暗号ファイルは、それを読み出す際には自動的に復号化され、平文ファイルが表示面HGに表示されまたはプリンタで印刷される。したがって、ユーザは、暗号ホルダFA内の暗号ファイルを通常のファイルと同じように閲覧し編集することができ、ファイルが暗号化されていることを全く意識する必要がない。

【0037】

暗号ホルダFAへの入出時のファイルの暗号化処理または復号化処理に用いられる鍵Kは、個別鍵KPが用いられる。

平文ホルダ F H は、一般的な O S またはアプリケーションの下で作成される通常の任意のホルダである。平文ホルダ F H には、暗号化されていない平文ファイルが格納される。但し、暗号ファイルをも格納することはできる。

【0038】

図4に破線で示すように、平文ホルダ F H 内の平文ファイルを暗号ホルダ F A 内に移動させると、個別鍵 K P による暗号化処理が行われ、暗号ホルダ F A には暗号ファイルが格納される。

【0039】

送受信ホルダ F T は、暗号通信に用いる送信用のファイルおよび受信した受信ファイルを格納するホルダである。一般の O S またはアプリケーションで提供されるホルダのうちのどれを送受信ホルダ F T に設定するかは、後で述べるようにユーザが選択することができる。送受信ホルダ F T に格納したファイルを送信するには、例えばそのファイルを電子メールの添付ファイルとすればよい。また、電子メールで受信したファイルが、この送受信ホルダ F T に入るように設定すればよい。

【0040】

暗号ホルダ F A に格納された暗号ファイルを送受信ホルダ F T に移動する際に、まず個別鍵 K P を用いて復号化処理 22 が行われ、続いて、復号化されたファイルに対し、グループ鍵 K G を用いて暗号化処理 21 が行われる。つまり、個別鍵 K P で暗号化されて暗号ホルダ F A に格納されていた暗号ファイルは、グループ鍵 K G で暗号化された暗号ファイルとして送受信ホルダ F T に格納される。なお、図には示されないが、復号化処理 22 および暗号化処理 21 のために、一時的なホルダが設けられる。

【0041】

また、平文ホルダ F H に格納された平文ファイルを送受信ホルダ F T に移動した際には、グループ鍵 K G を用いて暗号化処理 21 が行われる。つまり、個別鍵 K P で暗号化されて暗号ホルダ F A に格納されていた暗号ファイルは、グループ鍵 K G で暗号化された暗号ファイルとして送受信ホルダ F T に格納される。

【0042】

このように、暗号ホルダFAまたは平文ホルダFHのいずれに格納されていたファイルであっても、暗号化カードSPCを通過することにより、グループ鍵KGで暗号化された暗号ファイルが送受信ホルダFTに格納されることになる。したがって、暗号ファイルまたは平文ファイルのいずれであっても、それを電子メールの添付ファイルとする場合に、容易にグループ鍵KGで暗号化された暗号ファイルとすることができる。

【0043】

次に、受信側の通信端末5bは、暗号ホルダFA、平文ホルダFH、送受信ホルダFT、および暗号化カードSPCを有する。

暗号ホルダFA、平文ホルダFH、および送受信ホルダFTは、上にのべたと同様である。

【0044】

受信した電子メールまたはその添付ファイルが送受信ホルダFTに入ったとする。つまり、送受信ホルダFTには、グループ鍵KGで暗号化された暗号ファイルが格納される。

【0045】

送受信ホルダFTに格納された暗号ファイルを暗号ホルダFAに移動した際に、まずグループ鍵KGを用いて復号化処理22が行われ、続いて、復号化されたファイルに対し、個別鍵KPを用いて暗号化処理21が行われる。つまり、グループ鍵KGで暗号化されて送信され送受信ホルダFTに格納されていた暗号ファイルは、個別鍵KPで暗号化された暗号ファイルとして暗号ホルダFAに格納される。

【0046】

また、送受信ホルダFTから平文ホルダFHに移動した際には、グループ鍵KGを用いて復号化処理22が行われる。つまり、送受信ホルダFTに格納されていた暗号ファイルは、グループ鍵KGで復号化された平文ファイルとして平文ホルダFHに格納される。

【0047】

このように、送受信ホルダFTに格納された暗号ファイルは、暗号化カードS

PCを通過することにより、個別鍵KPで暗号化された暗号ファイルとして暗号ホルダFAに格納され、または平文ファイルとして平文ホルダFHに格納されることとなる。

【0048】

なお、各通信端末5において、暗号化カードSPCの使用に先立って、ユーザIDおよびグループIDを入力して個別鍵KPおよびグループ鍵KGを選択し、それらを活性化しておく必要がある。

【0049】

次に、通信端末5における処理をフローチャートおよび画面を参照してさらに詳しく説明する。

図5は個別セキュリティの処理を示すフローチャート、図6は通信セキュリティの処理を示すフローチャート、図7は暗号送信処理を示すフローチャート、図8は暗号受信処理を示すフローチャート、図9はグループ鍵での復号化処理を示すフローチャート、図10は個別ID認証画面HG1を示す図、図11は個別鍵KPが活性化された状態の画面HG2を示す図、図12は暗号通信のためのプルダウンメニューの画面HG3を示す図、図13はグループID認証画面HG4を示す図、図14は送信時における送信ファイルの選択の状態を示す図、図15は受信時における受信ファイルの状態を示す図である。

【0050】

図5に示す個別セキュリティは、通信を行うことなく、通信端末5の内部において個別鍵KPのみを用いてファイルのセキュリティを確保するために必要な前処理である。

【0051】

すなわち、暗号通信のためのアプリケーション（または個別セキュリティのためのアプリケーション）を立ち上げると、まず最初に図10に示す個別ID認証画面HG1が表示されるので、個別ID（ユーザID）およびパスワードを入力し、「OK」ボタンを押す（クリックする）（#11）。

【0052】

そうすると、入力された個別IDおよびパスワードの認証が行われる（#12

）。認証がOKであれば、その個別IDに対応する個別鍵KPが有効となる（#13）。したがって、同じ通信端末5であっても、ユーザ毎に個別IDおよびパスワードを設定しておくことによって、複数のユーザがそれぞれのセキュリティを確保することができる。

【0053】

図11に示すように、個別鍵KPが有効となったことを示す鍵マークを示す画面HG2が表示され（#14）、暗号ホルダFAが活性化される（#15）。

図6に示す通信セキュリティは、暗号通信を行うに必要な前処理である。

【0054】

図11に示す画面HG2の鍵マークを右クリックすると、図12に示すように、暗号通信のためのプルダウンメニューを示す画面HG3が表示される。ここで「暗号通信」をクリックすると、図13に示すグループID認証画面HG4が表示される。そこで、グループIDおよびパスワードを入力し、「OK」ボタンを押す（#21）。

【0055】

そうすると、入力されたグループIDおよびパスワードの認証が行われる（#22）。認証がOKであれば、そのグループIDに対応するグループ鍵KGが有効となる（#23）。これとともに、次の画面HG5～8が表示される。

【0056】

なお、グループIDを入力する際に、送信先に応じたグループIDを入力するようにすればよい。つまり、複数の送信先を予め設定しておき、且つ送信先に応じて異なるグループIDを割り当てておく。そして、各送信先においても、同じグループIDを用いることに決めておく。これによって、通信の予定された2つまたは3つ以上の通信端末5間において、且つそれらの通信端末5間においてのみ、同じグループIDつまり同じグループ鍵KGが用いられることとなり、セキュリティの維持が確実となる。

【0057】

図6において、送信する場合には（#24でイエス）、暗号送信処理が行われ（#25）、受信する場合には（#26でイエス）、暗号受信処理が行われ（#

27)。

【0058】

図7において、暗号送信処理では、まず、送信ファイルの選択が行われる（#31）。

すなわち、図14（A）に示す画面HG5において、左側に運用ホルダFUが、右側に送受信ホルダFTが表示され、それぞれの上に参照ボタンBT3，4が表示され、中央にそれらの間の変換を指示する変換ボタンBT1，2が表示される。

【0059】

参照ボタンBT3を押すと、ホルダのリストが表示されるので、その中から運用ホルダFUとして設定するホルダを選択する。

参照ボタンBT4を押すと、ホルダのリストが表示されるので、その中から送受信ホルダFTとして設定するホルダを選択する。

【0060】

図14（B）に示す状態では、運用ホルダFUには「○×.doc」および「△□.doc」の2つのファイル（平文ファイル）が格納されている。ここで、変換ボタンBT1を押すと、図14（C）に示すように、それらのファイルに対する暗号化処理が行われるとともに、ファイルは運用ホルダFUから送受信ホルダFTに移動し、運用ホルダFU内にあったファイルは削除される。

【0061】

すなわち、図7において、運用ホルダFUのファイルが暗号ファイルであった場合には（#32でイエス）、個別鍵KPで復号化し（#33）、続いてグループ鍵KGで暗号化する（#34）。運用ホルダFUのファイルが暗号ファイルでなかった場合には（#32でノー）、そのままグループ鍵KGで暗号化する（#34）。

【0062】

グループ鍵KGによる暗号化の際に、元のファイルのファイル識別子がファイル名に組み込まれ、暗号化されたファイルであることを示す識別子が新たに付加される。また、グループ鍵KGに対応するグループIDが、属性情報としてヘッ

ダに書き込まれる。

【0063】

図14 (B) (C) に示す例では、ファイル名「O×. doc」がファイル名「O×doc. enc」と変更されている。つまり、元のファイルのファイル識別子「doc」がファイル名に組み込まれて「O×doc」となり、暗号化されたファイルであることを示す識別子「enc」が新たに付加されている。

【0064】

なお、暗号化されたファイルであることを示す識別子に、グループIDを示す符号を付加しておくことも可能である。

図8において、暗号受信処理では、まず、受信ファイルの選択が行われる（#41）。

【0065】

すなわち、図15に示す画面HG8において、参照ボタンBT4を押すと、ホルダのリストが表示されるので、その中から送受信ホルダFTとして設定するホルダを選択する。

【0066】

参照ボタンBT3を押すと、ホルダのリストが表示されるので、その中から運用ホルダFUとして設定するホルダを選択する。

図15に示す状態では、送受信ホルダFTには「O×doc. enc」および「△□doc. enc」の2つのファイルが格納されている。ここで、変換ボタンBT2を押すと、それらのファイルに対する復号化処理が行われるとともに、ファイルは送受信ホルダFTから運用ホルダFUに移動し、送受信ホルダFT内にあったファイルは削除される。

【0067】

すなわち、図8において、送受信ホルダFT内のファイルがグループ鍵KGで復号化される（#42）。格納先のホルダ（運用ホルダFU）が暗号ホルダFAであった場合には（#43でイエス）、さらに個別鍵KPで暗号化され（#44）、その後、平文ファイルが削除される（#45）。

【0068】

なお、復号化を行った後で受信したファイル自体を自動的に削除するか否かについて、ユーザが設定することができる。また、図15に示す送受信ホルダFTに、識別子が「enc」でないファイルが格納された場合には、その旨の警報が表示される。

【0069】

図9において、グループ鍵KGでの復号化処理では、対象となるファイルのヘッダのグループIDが抽出される(#51)。そして、抽出されたグループIDと、予め認証のために入力されたグループIDとが比較され、認証済のグループ鍵KGが正しいか否かが判断される(#52)。合っていない場合に、グループIDの再入力などを行う(#53)。

【0070】

そして、ヘッダを除去し(#54)、グループ鍵KGを復号化を行い(#55)、ファイル名を復元する(#56)。

なお、受信側において、使用可能なグループ鍵KGが複数個ある場合に、受信したファイルのヘッダから抽出されたグループIDによって使用するグループ鍵KGを自動的に選択するようにしてもよい。このようにすると、グループ鍵KGの異なる複数の送信側から送られた暗号ファイルを受信した際に、受信側においてそれぞれのグループ鍵KGを自動的に選択して復号化を行うことが可能となる。

【0071】

次に、暗号通信のための操作方法の異なる他の実施形態について説明する。

図16は他の実施形態を示す送信ファイルの選択処理のフローチャート、図17はファイル選択のメイン画面HG21を示す図である。

【0072】

個別セキュリティのためのアプリケーションが立ち上がった状態で、つまり個別IDの認証が終了している状態で、暗号通信のためのアプリケーションを立ち上げると、まず最初に図17に示すメイン画面HG21が表示される。

【0073】

メイン画面HG21では、ファイル選択ボタンBT21、暗号化ボタンBT2

2、復号化ボタンBT23、オプションボタンBT24、リスト表示欄FC、および図示しないプログレスバーが表示される。

【0074】

ファイル選択ボタンBT21を押すと、Windows 標準のファイル選択画面が表示されるので、その中から暗号化または復号化の対象となるファイルを選択する。選択したファイル名がリスト表示欄FCに表示される（#101）。

【0075】

暗号化ボタンBT22を押すと、図13に示すグループID認証画面HG4が表示されるので、グループIDおよびパスワードを入力し、「OK」ボタンを押す（#102）。入力されたグループIDおよびパスワードの認証が行われ（#103）、認証がOKであれば、そのグループIDに対応するグループ鍵KGが有効となる（#104）。

【0076】

これとともに、暗号ファイルの格納先を選択する画面が表示されるので、適当な格納先を指定する（#105）。対象となるファイルが暗号ファイルであった場合には（#106でイエス）、個別鍵KPで復号化した後（#107）、グループ鍵KGで暗号化を行う（#108）。暗号ファイルでない場合には、そのままグループ鍵KGで暗号化を行う（#108）。

【0077】

上に述べた通信システム1によると、暗号化されたファイルおよび暗号化されていないファイルが混在している場合でも、容易な操作で間違うことなく暗号通信を行うことができる。

【0078】

上の実施形態において、通信端末5として、パームトップ型、ノート型、ラップトップ型、デスクトップ型、その他の種々の形式のパーソナルコンピュータまたは情報端末を用いることができる。

【0079】

上の実施形態においては、送信側および受信側において、少なくとも1つの共通のグループ鍵KGを準備しておくいわば共通鍵暗号方式の場合を説明したが、

送信側と受信側とで共通の鍵Kを準備することなく、互いに異なる鍵を用いて暗号化と復号化とを行うようにしてもよい。また、例えば、公開鍵暗号方式を採用する場合には、暗号化を行う鍵を公開し、復号化を行う鍵のみを秘密にしておけばよい。その他、通信システム1の全体または各部の構成、処理の内容、順序、および画面の構成などは、本発明の趣旨に沿って適宜変更することができる。

【0080】

【発明の効果】

本発明によると、暗号化されたファイルおよび暗号化されていないファイルを混在して扱う場合などにおいても、容易な操作で間違うことなく暗号通信を行うことができる。

【図面の簡単な説明】

【図1】

通信システムの例を示すブロック図である。

【図2】

暗号化カードの構成を示すブロック図である。

【図3】

グループ鍵により暗号化処理を行った際のファイルの状態の変化を示す図である。

【図4】

通信端末の暗号通信時における機能を示すブロック図である。

【図5】

個別セキュリティの処理を示すフローチャートである。

【図6】

通信セキュリティの処理を示すフローチャートである。

【図7】

暗号送信処理を示すフローチャートである。

【図8】

暗号受信処理を示すフローチャートである。

【図9】

グループ鍵での復号化処理を示すフローチャートである。

【図 10】

個別 I D 認証画面を示す図である。

【図 11】

個別鍵が活性化された状態を示す画面である。

【図 12】

暗号通信のためのプルダウンメニューを示す画面である。

【図 13】

グループ I D 認証画面を示す図である。

【図 14】

送信時における送信ファイルの選択の状態を示す図である。

【図 15】

受信時における受信ファイルの状態を示す図である。

【図 16】

他の実施形態を示す送信ファイルの選択処理のフローチャートである。

【図 17】

ファイル選択のメイン画面を示す図である。

【符号の説明】

1 通信システム

5 通信端末（ファイルアクセスシステム）

11 処理装置

S P C 暗号化カード（暗号化処理装置）

K 鍵

K P 個別鍵（個別用の鍵、一方の鍵、第 1 の鍵）

K G グループ鍵（通信用の鍵、他方の鍵、第 2 の鍵）

F U 運用ホルダ（第 1 のホルダ）

F T 送受信ホルダ（第 2 のホルダ）

C D C D-R O M（記録媒体）

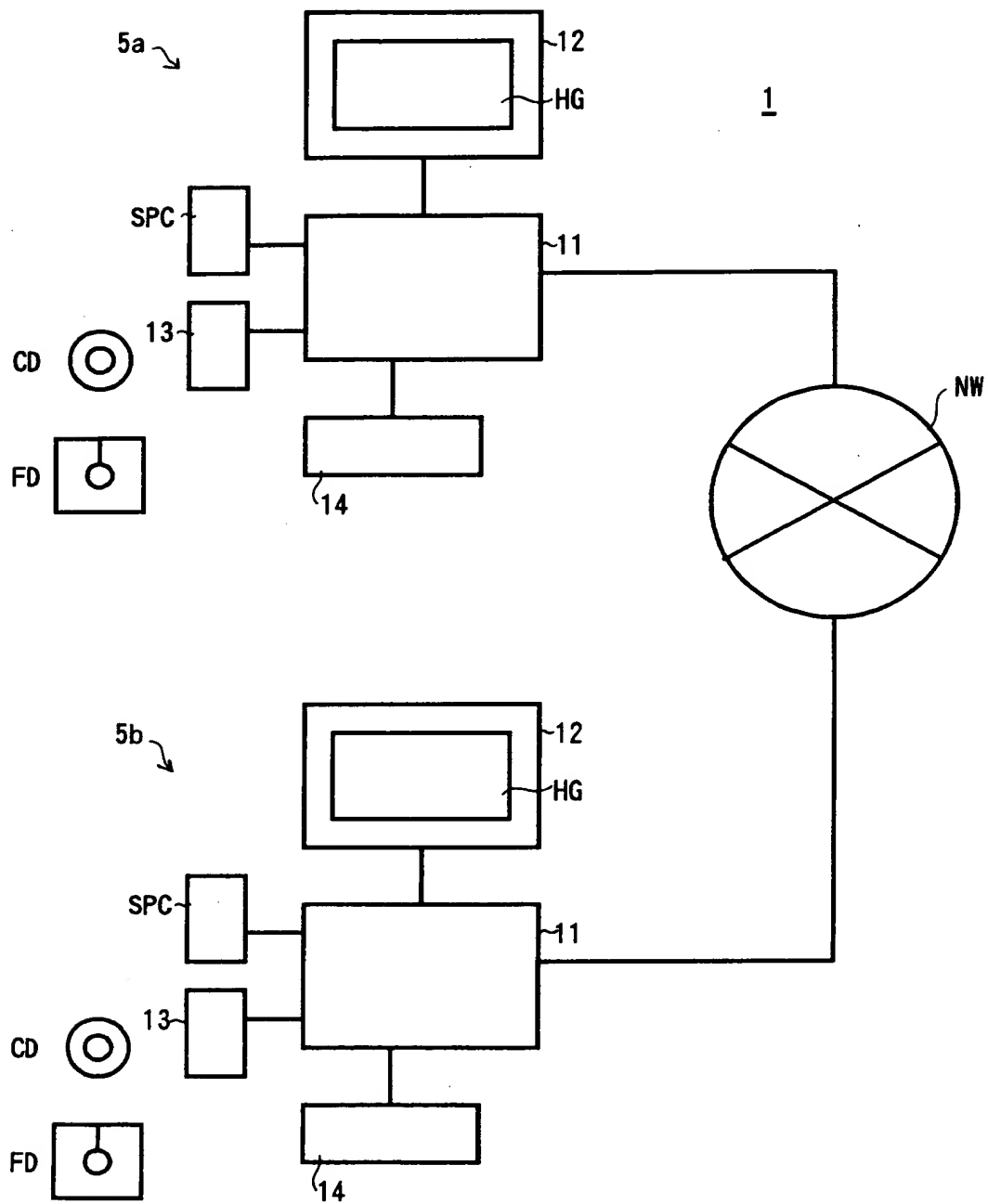
F D フロッピーディスク（記録媒体）

特 2 0 0 0 - 0 1 6 6 5 7

【書類名】 図面

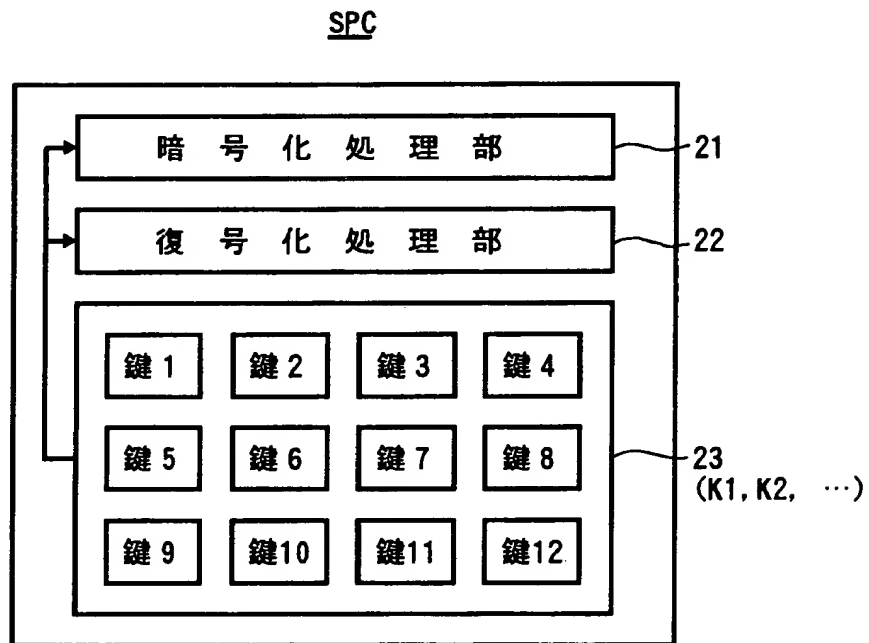
【図 1】

通信システムの例を示すブロック図



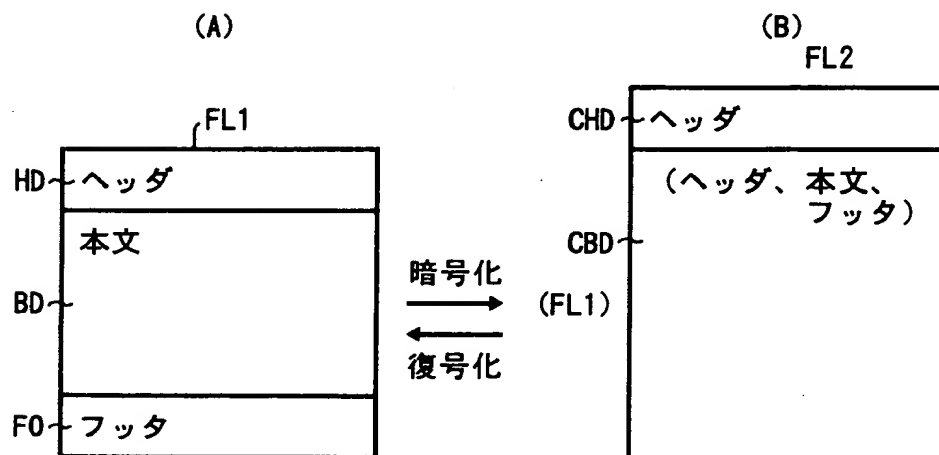
【図 2】

暗号化カードの構成を示すブロック図



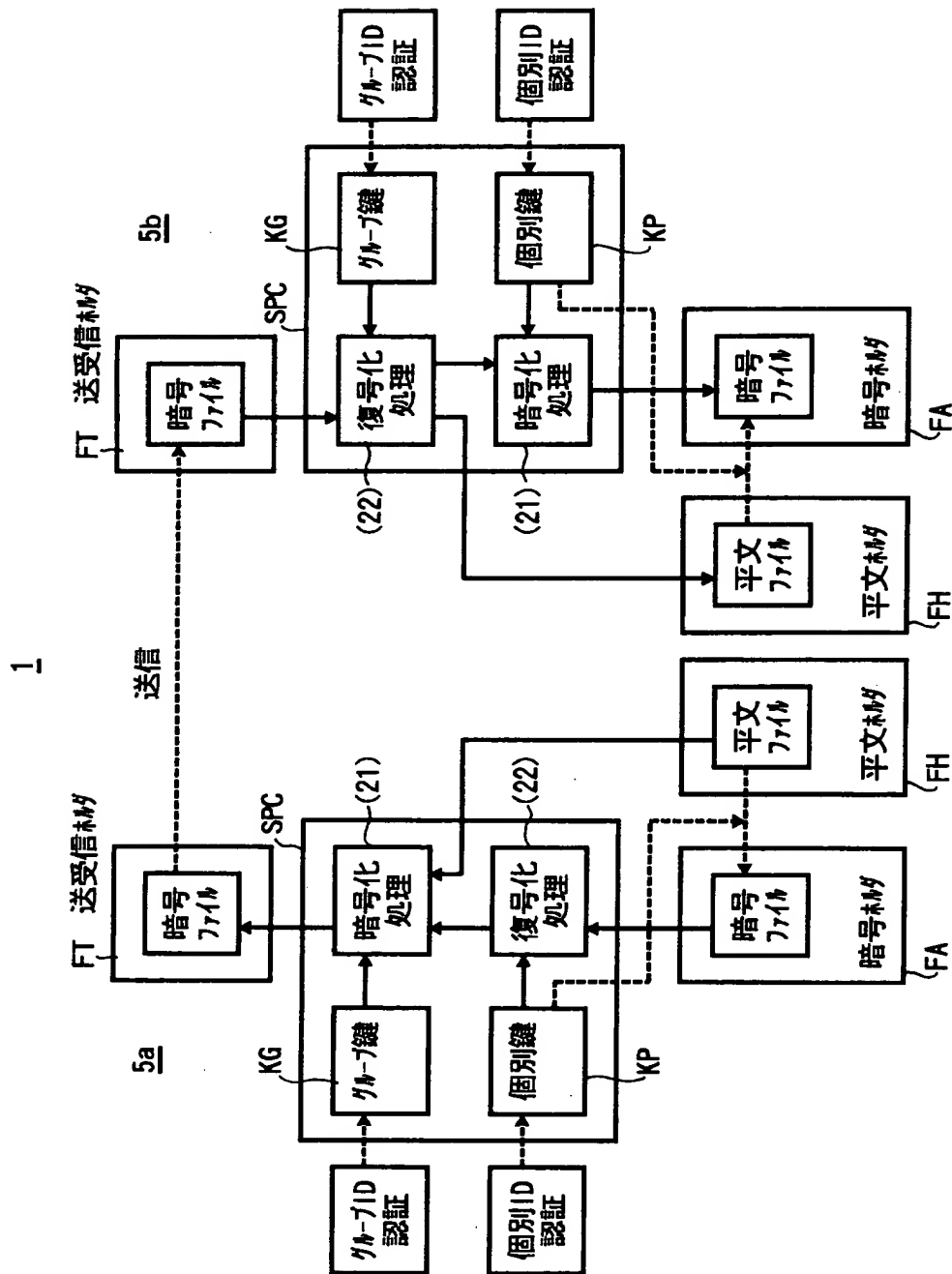
【図 3】

グループ鍵により暗号化処理を行った際のファイルの状態の変化を示す図



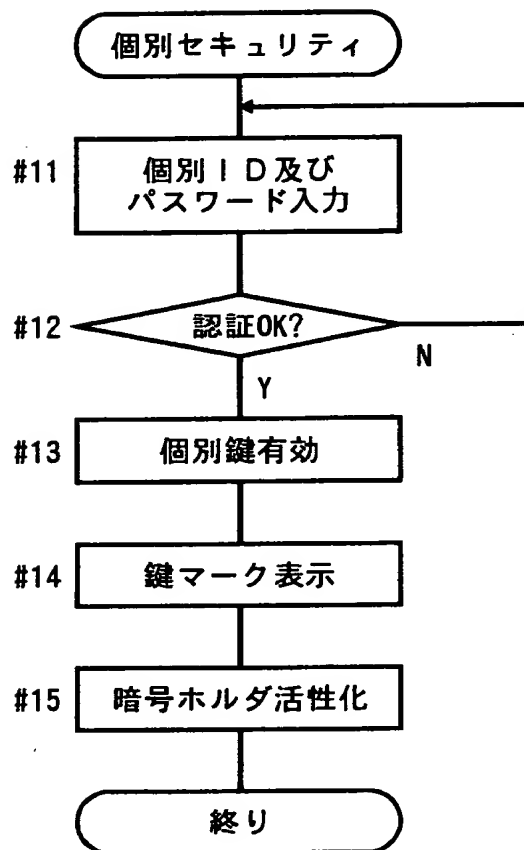
【図 4】

通信端末の暗号通信時における機能を示すブロック図



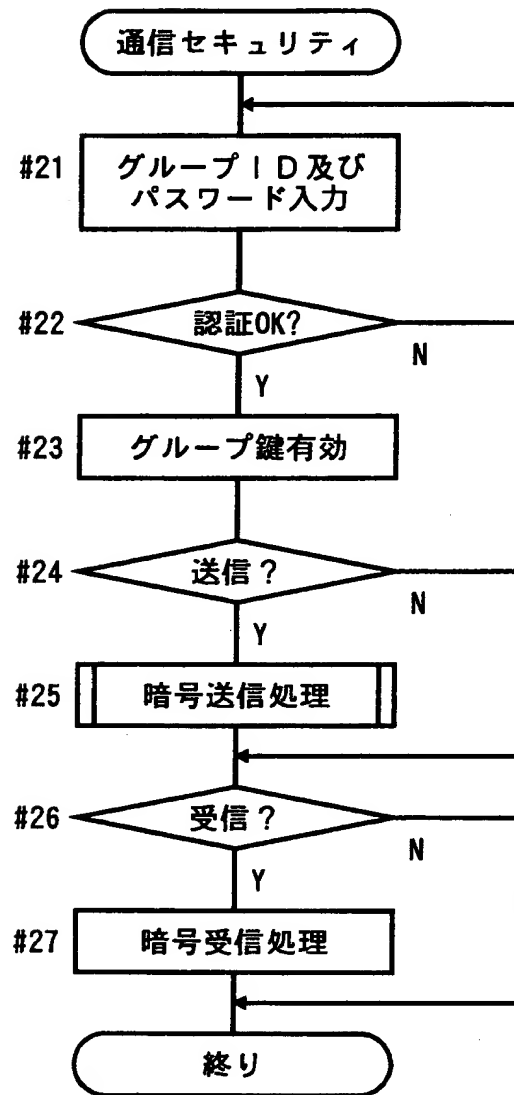
【図 5】

個別セキュリティの処理を示すフローチャート



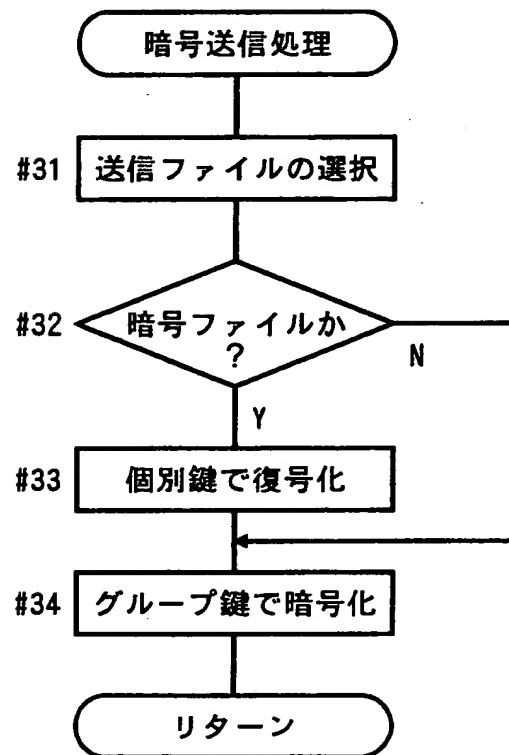
【図 6】

通信セキュリティの処理を示すフローチャート



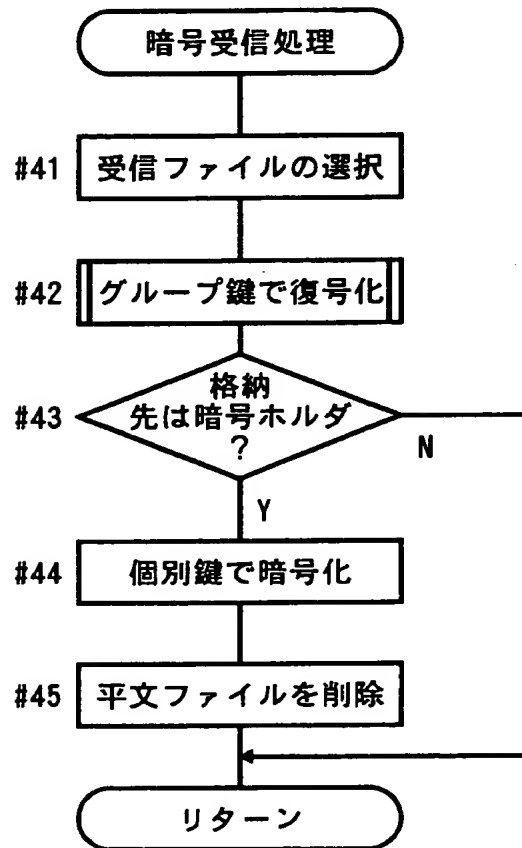
【図 7】

暗号送信処理を示すフローチャート



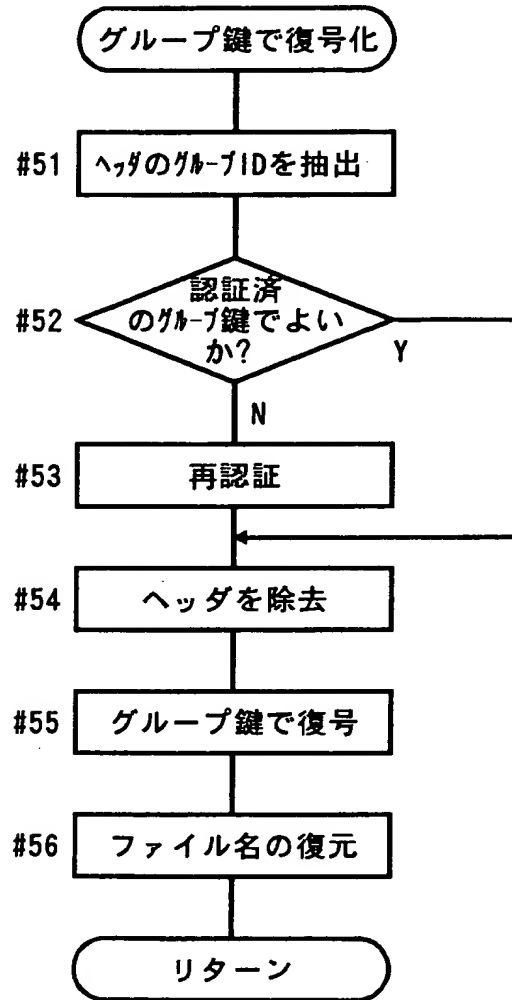
【図 8】

暗号受信処理を示すフローチャート



【図9】

グループ鍵での復号化処理を示すフローチャート



【図 1 0】

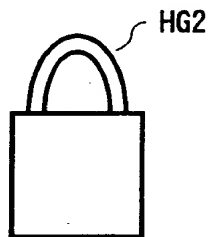
個別 I D 認証画面を示す図

HG1

ユーザ I D	<input type="text"/>	OK
パスワード	<input type="text"/>	キャンセル

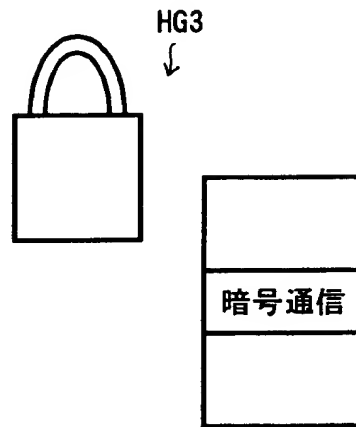
【図 1 1】

個別鍵が活性化された状態を示す画面



【図 1 2】

暗号通信のためのプルダウンメニューを示す画面



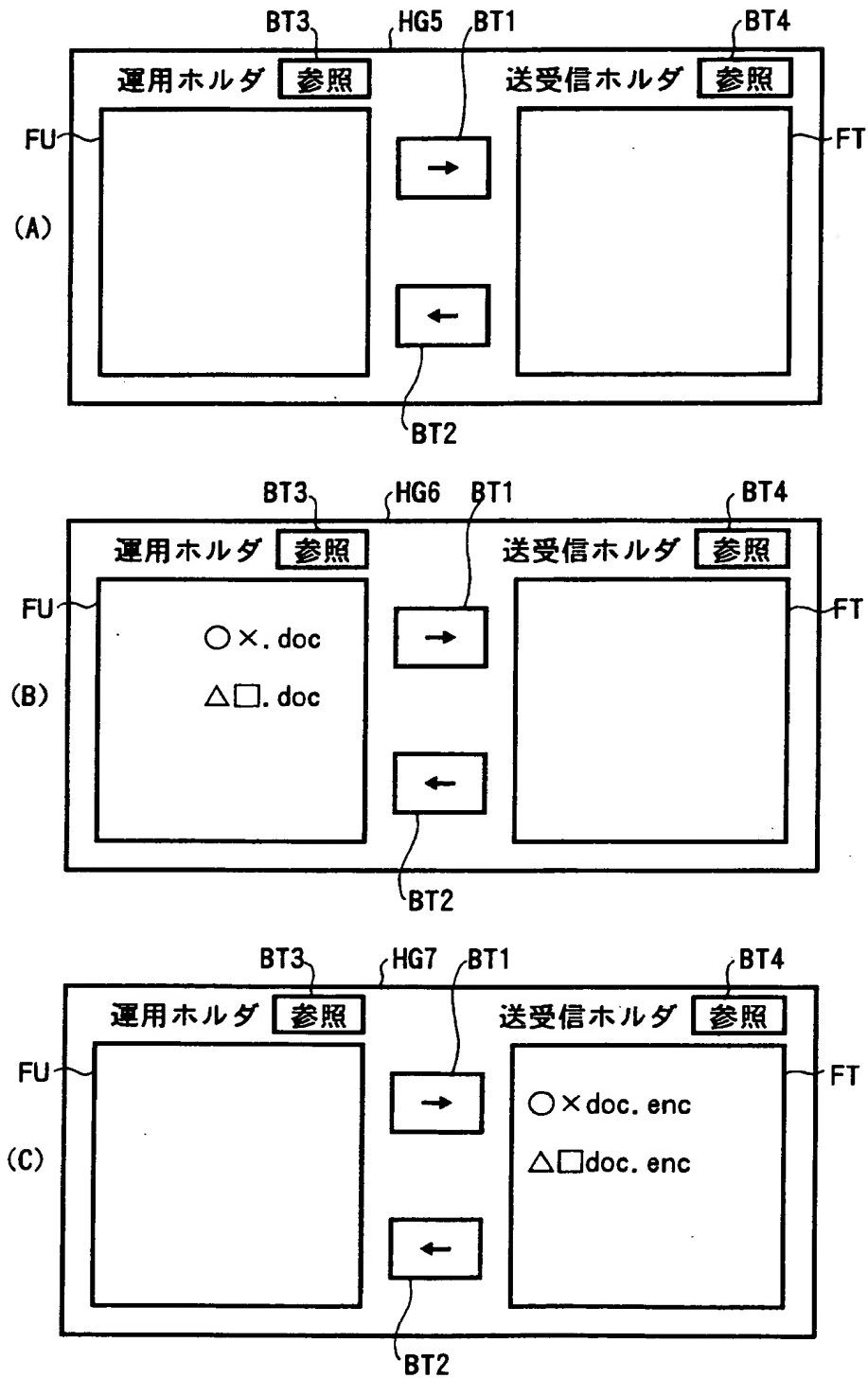
【図 1 3】

グループID認証画面を示す図

The diagram shows a rectangular frame representing a screen. At the top center, the label "HG4" is present with a bracket. Inside the frame, on the left side, are two input fields. The top field is preceded by the text "グループID" (Group ID), and the bottom field is preceded by "パスワード" (Password). On the right side of the frame, there are two buttons: the top one is labeled "OK" and the bottom one is labeled "キャンセル" (Cancel).

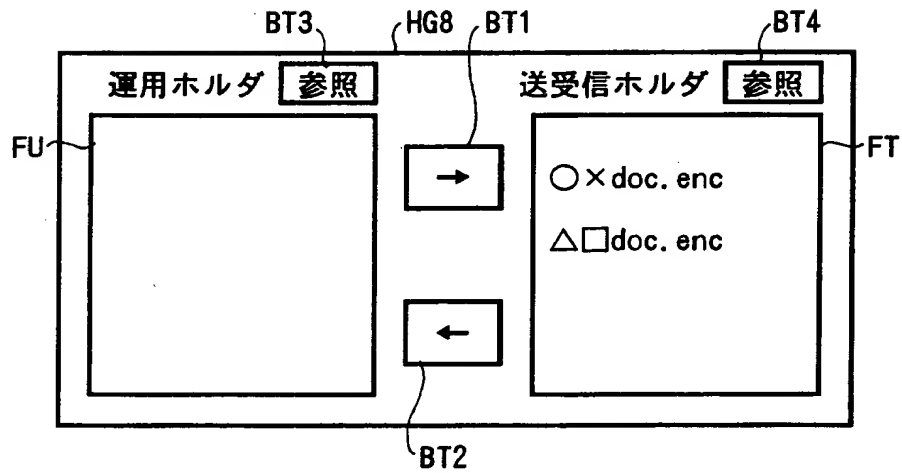
【図 14】

送信時における送信ファイルの選択の状態を示す図



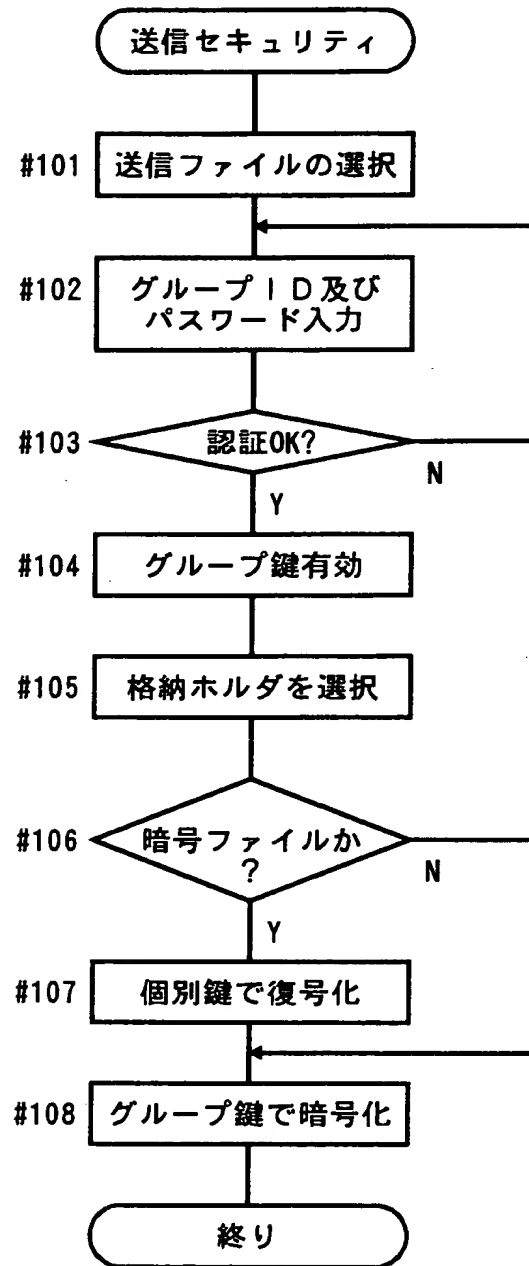
【図 15】

受信時における受信ファイルの状態を示す図



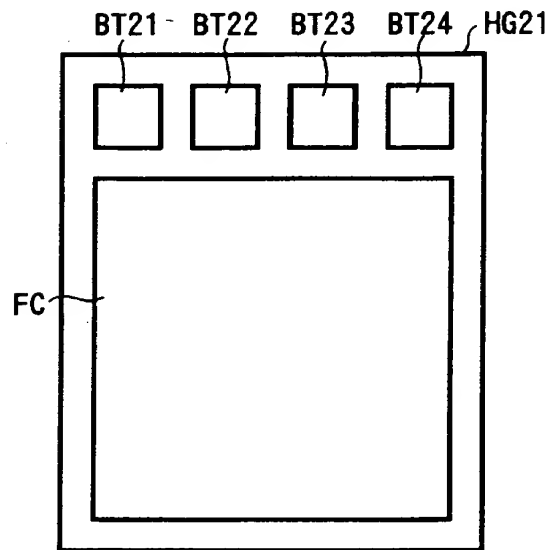
【図16】

他の実施形態を示す送信ファイルの選択処理のフローチャート



【図 1 7】

ファイル選択のメイン画面を示す図



【書類名】 要約書

【要約】

【課題】暗号化されたデータおよび暗号化されていないデータを混在して扱う場合などにおいて、容易な操作で間違うことなく暗号通信を行えるようにすること

【解決手段】送信側において通信用の鍵を用いてデータを暗号化して送信し、受信側において受信したデータを送信側と共通の通信用の鍵を用いて復号化する暗号通信方法であって、送信側において、通信用の鍵とは異なる個別用の鍵で暗号化されたデータを送信するに当たり、暗号化されたデータを、個別用の鍵を用いて復号化し、続いて、復号化されたデータを通信用の鍵を用いて暗号化して送信する。

【選択図】 図 7

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社